AMENDMENTS TO CLAIMS

Claim 1 (currently amended): A digital signature cryptographic method comprising:

supplying a set S1 of k polynomial functions as a public-key, the set S1 including the functions $P_1(x_1,...,x_{n+v}, y_1,\dots,y_k),\dots, P_k(x_1,...,x_{n+v}, y_1,\dots,y_k)$, where k, v, and n are integers, $x_1,...,x_{n+v}$ are n+v variables of a first type, $y_1,\dots,y_k$ are k variables of a second type, and the set S1 is obtained by applying a secret key operation on a set S2 of k polynomial functions $P'_1(a_1,...,a_{n+v},y_1,\dots,y_k),\dots,P'_k(a_1,...,a_{n+v},y_1,\dots,y_k)$ where $a_1,...,a_{n+v}$ are n+v variables which include a set of n "oil" variables $a_1,...,a_n$, and a set of v "vinegar" variables $a_{n+1},...,a_{n+v}$, the supplying comprising selecting the number v of "vinegar" variables to be greater than the number n of "oil" variables;

providing a message to be signed;

applying a hash function on the message to produce a series of k values $b_1,\dots,b_k$;

C1

substituting the series of k values $b_1,\dots,b_k$ for the variables $y_1,\dots,y_k$ of the set S2 respectively to produce a set S3 of k polynomial functions $P''_1(a_1,...,a_{n+v}),\dots, P''_k(a_1,...,a_{n+v})$;

selecting v values $a'_{n+1},...,a'_{n+v}$ for the v "vinegar" variables $a_{n+1},\dots,a_{n+v}$;

solving a set of equations $P''_1(a_1,...,a_n,a'_{n+1},...,a'_{n+v})=0,\dots, P''_k(a_1,...,a_n,a'_{n+1},...,a'_{n+v})=0$ to obtain a solution for $a'_1,...,a'_n$; and

applying the secret key operation to transform $a'_1,...,a'_{n+v}$ to a digital signature $e_1,...,e_{n+v}$.

Claim 2 (previously presented): A method according to claim 1 and also comprising verifying the digital signature.

Claim 3 (previously presented): A method according to claim 2 and wherein said verifying comprises:

obtaining the signature $e_1,...,e_{n+v}$, the message, the hash function and the public key;

applying the hash function on the message to produce the series of k values $b_1,\ldots,b_k$; and

verifying that the equations $P_1(e_1,...,e_{n+v},b_1,\ldots,b_k)=0,\ldots, P_k(e_1,...,e_{n+v}, b_1,\ldots,b_k)=0$ are satisfied.

Claim 4 (previously presented): A method according to claim 1 and wherein the method comprises an HFEV scheme and the set S2 comprises a set f(a) of k polynomial functions of the HFEV scheme.

Claim 5 (previously presented): A method according to claim 1 and wherein the method comprises a UOV scheme and the set S2 comprises a set S of k polynomial functions of the UOV scheme.

C1

Claim 6 (canceled)

Claim 7 (previously presented): A method according to claim 1 and wherein v is selected such that q^v is greater than 2^{32}, where q is the number of elements of a finite field K over which the sets S1, S2 and S3 are provided.

Claim 8 (previously presented): A method according to claim 1 and wherein said supplying comprises obtaining the set S1 from a subset S2' of k polynomial functions of the set S2, the subset S2' being characterized in that all coefficients of components involving any of the $y_1,\ldots,y_k$ variables in the k polynomial functions $P'_1(a_1,...,a_{n+v},y_1,\ldots,y_k),\ldots,P'_k(a_1,...,a_{n+v},y_1,\ldots,y_k)$ are zero, and the number v of "vinegar" variables is greater than the number n of "oil" variables.

Claim 9 (previously presented): A method according to claim 8 and wherein the set S2 comprises a set S of k polynomial functions of a UOV scheme, and the number v of "vinegar" variables is selected to satisfy one of the following conditions:

(a) for each characteristic p other than 2 of a field K in an “Oil and Vinegar” scheme of degree 2, v satisfies the inequality $q^{(v-n)-1} * n^4 > 2^{40}$, where K is a finite field over which the sets S1, S2 and S3 are provided,

(b) for p = 2 in an “Oil and Vinegar” scheme of degree 3, v is greater than $n*(1 + \mathrm{sqrt}(3))$ and less than or equal to $n^3/6$, and

(c) for each p other than 2 in an “Oil and Vinegar” scheme of degree 3, v is greater than n and less than or equal to n^4.

Claim 10 (previously presented): A method according to claim 8 and wherein the set S2 comprises a set S of k polynomial functions of a UOV scheme, and the number v of “vinegar” variables is selected to satisfy the inequalities $v<n^2$ and $q^{(v-n)-1} * n^4 >2^{40}$ for a characteristic p=2 of a field K in an “Oil and Vinegar” scheme of degree 2, where K is a finite field over which the sets S1, S2 and S3 are provided and q is the number of elements of K.

C1

Claim 11 (original): A method according to claim 1 and wherein said secret key operation comprises a secret affine transformation s on the n+v variables $a_1,\ldots,a_{n+v}$.

Claim 12 (original): A method according to claim 4 and wherein said set S2 comprises an expression including k functions that are derived from a univariate polynomial.

Claim 13 (original): A method according to claim 12 and wherein said univariate polynomial includes a univariate polynomial of degree less than or equal to 100,000.

Claim 14 (original): A cryptographic method for verifying the digital signature of claim 1, the method comprising:

obtaining the signature $e_1,\ldots,e_{n+v}$, the message, the hash function and the public key;

applying the hash function on the message to produce the series of k values $b_1,\ldots,b_k$; and

verifying that the equations $P_1(e_1,\ldots,e_{n+v},b_1,\ldots,b_k)=0,\ldots,$ $P_k(e_1,\ldots,e_{n+v},$ $b_1,\ldots,b_k)=0$ are satisfied.

Claim 15 (previously presented): In an "Oil and Vinegar" signature method, an improvement comprising using more "vinegar" variables than "oil" variables.

Claim 16 (previously presented): A method according to claim 15 and wherein a number v of "vinegar" variables is selected to satisfy one of the following conditions:

(a) for each characteristic p other than 2 of a field K and for a degree 2 of the "Oil and Vinegar" signature method, v satisfies the inequality $q^{(v-n)-1} * n^4 > 2^{40}$, where n is a number of "oil" variables, K is a finite field from which the n "oil" variables and the v "vinegar" variables are selected, and q is the number of elements of K,

C 1

(b) for p = 2 and for a degree 3 of the "Oil and Vinegar" signature method, v is greater than n*(1 + sqrt(3)) and less than or equal to $n^3/6$, and

(c) for each p other than 2 and for a degree 3 of the "Oil and Vinegar" signature method, v is greater than n and less than or equal to n^4.

Claim 17 (previously presented): A method according to claim 15 and wherein a number v of "vinegar" variables is selected to satisfy the inequalities $v<n^2$ and $q^{(v-n)-1} * n^4 >2^{40}$ for a characteristic p=2 of a field K in an "Oil and Vinegar" scheme of degree 2, where n is a number of "oil" variables, K is a finite field from which the n "oil" variables and the v "vinegar" variables are selected, and q is the number of elements of K.

Claim 18 (currently amended): A signature generator comprising:

a signature input receiver operative to receive a set S1 of k polynomial functions as a public-key and a message to be signed, the set S1 including the functions $P_1(x_1,...,x_{n+v}, y_1,...,y_k),..., P_k(x_1,...,x_{n+v}, y_1,...,y_k)$, where k, v, and n are integers, $x_1,...,x_{n+v}$ are n+v variables of a first type, $y_1,...,y_k$ are k variables of a second type, and the set S1 is obtained by applying a secret key operation on a set S2 of k polynomial functions $P'_1(a_1,...,a_{n+v},y_1,...,y_k),...,P'_k(a_1,...,a_{n+v},y_1,...,y_k)$, where $a_1,...,a_{n+v}$ are n+v variables which include a set of n "oil" variables $a_1,...,a_n$, and a set of v "vinegar" variables $a_{n+1},...,a_{n+v}$ and the number v of "vinegar" variables is greater than the number n of "oil" variables; and

a signature processor operatively associated with the signature input receiver and operative to perform the following operations:

to apply a hash function on the message to produce a series of k values $b_1,...,b_k$,

to substitute the series of k values $b_1,...,b_k$ for the variables $y_1,...,y_k$ of the set S2 respectively to produce a set S3 of k polynomial functions $P''_1(a_1,...,a_{n+v}),..., P''_k(a_1,...,a_{n+v})$,

C1

to select v values $a'_{n+1},...,a'_{n+v}$ for the v "vinegar" variables $a_{n+1},...,a_{n+v}$;

to solve a set of equations $P''_1(a_1,...,a_n,a'_{n+1},...,a'_{n+v})=0,..., P''_k(a_1,...,a_n,a'_{n+1},...,a'_{n+v})=0$ to obtain a solution for $a'_1,...,a'_n$; and

to apply the secret key operation to transform $a'_1,...,a'_{n+v}$ into a digital signature $e_1,...,e_{n+v}$.

Claim 19 (previously presented): Apparatus according to claim 18 and also comprising a signature verifier operatively associated with the signature processor and operative to verify the digital signature.

Claim 20 (previously presented): Apparatus according to claim 19 and wherein said signature verifier is operative to verify the digital signature by performing the following operations:

obtaining the signature $e_1,...,e_{n+v}$, the message, the hash function and the public key;

applying the hash function on the message to produce the series of k values $b_1,\ldots,b_k$; and

verifying that the equations $P_1(e_1,...,e_{n+v},b_1,\ldots,b_k)=0,\ldots,\ P_k(e_1,...,e_{n+v}, b_1,\ldots,b_k)=0$ are satisfied.

Claim 21 (previously presented): Apparatus according to claim 18 and wherein the signature processor is operative to perform an HFEV scheme, and the set S2 comprises a set f(a) of k polynomial functions of the HFEV scheme.

Claim 22 (previously presented): Apparatus according to claim 18 and wherein the signature processor is operative to perform a UOV scheme, and the set S2 comprises a set S of k polynomial functions of the UOV scheme.

C1

Claim 23 (canceled)

Claim 24 (previously presented): Apparatus according to claim 18 and wherein v is selected such that q^v is greater than 2^{32}, where q is the number of elements of a finite field K over which the sets S1, S2 and S3 are provided.

Claim 25 (previously presented): Apparatus according to claim 18 and wherein the set S1 is obtained from a subset S2' of k polynomial functions of the set S2, the subset S2' being characterized in that all coefficients of components involving any of the $y_1,\ldots,y_k$ variables in the k polynomial functions $P'_1(a_1,...,a_{n+v},y_1,\ldots,y_k), \ldots,P'_k(a_1,...,a_{n+v},y_1,\ldots,y_k)$ are zero, and the number v of "vinegar" variables is greater than the number n of "oil" variables.

Claim 26 (previously presented): Apparatus according to claim 25 and wherein the set S2 comprises a set S of k polynomial functions of a UOV scheme, and the number v of "vinegar" variables is selected to satisfy one of the following conditions:

(a) for each characteristic p other than 2 of a field K in an "Oil and Vinegar" scheme of degree 2, v satisfies the inequality $q^{(v-n)-1} * n^4 > 2^{40}$, where K is a finite field over which the sets S1, S2 and S3 are provided,

(b) for p = 2 in an "Oil and Vinegar" scheme of degree 3, v is greater than n*(1 + sqrt(3)) and less than or equal to $n^3/6$, and

(c) for each p other than 2 in an "Oil and Vinegar" scheme of degree 3, v is greater than n and less than or equal to n^4.

C1

Claim 27 (currently amended): Apparatus according to claim 25 and wherein the set S2 comprises a set S of k polynomial functions of a UOV scheme, and the number v of "vinegar" variables is selected to satisfy the inequalities $v<n^2$ and $q^{(v-n)-1} * n^4 >2^{40}$ for a characteristic p=2 of a field K in an "Oil and Vinegar" scheme of degree 2, [[2,]] where K is a finite field over which the sets S1, S2 and S3 are provided and q is the number of elements of K.

Claim 28 (previously presented): Apparatus according to claim 18 and wherein said secret key operation comprises a secret affine transformation s on the n+v variables $a_1,\dots,a_{n+v}$.

Claim 29 (previously presented): Apparatus according to claim 21 and wherein said set S2 comprises an expression including k functions that are derived from a univariate polynomial.

Claim 30 (previously presented): Apparatus according to claim 29 and wherein said univariate polynomial includes a univariate polynomial of degree less than or equal to 100,000.

Claim 31 (previously presented): A signature verifier for verifying the digital signature generated by the signature generator of claim 18, the signature verifier comprising a verifier processor operative to perform the following operations:

to obtain the signature $e_1,...,e_{n+v}$, the message, the hash function and the public key via the signature input receiver;

to apply the hash function on the message to produce the series of k values $b_1,\ldots,b_k$; and

to verify that the equations $P_1(e_1,...,e_{n+v},b_1,\ldots,b_k)=0,\ldots, P_k(e_1,...,e_{n+v}, b_1,\ldots,b_k)=0$ are satisfied.

Claim 32 (previously presented): In an "Oil and Vinegar" signature generating apparatus an improvement characterized in that the "Oil and Vinegar" signature generating apparatus is operative to use more "vinegar" variables than "oil" variables.

C1

Claim 33 (currently amended): An "Oil and Vinegar" signature generating apparatus according to claim 32 and wherein a number v of "vinegar" variables is selected to satisfy one of the following conditions:

(a) for each characteristic p other than 2 of a field K and for a degree 2 of an "Oil and Vinegar" signature method, v satisfies the <u>inequality</u> $q^{(v-n)-1} * n^4 > 2^{40}$, where n is a number of "oil" variables, K is a finite field from which the n "oil" variables and the v "vinegar" variables are selected, and q is the number of elements of K,

(b) for p = 2 and for a degree 3 of the "Oil and Vinegar" signature method, v is greater than $n*(1 + \mathrm{sqrt}(3))$ and less than or equal to $n^3/6$, and

(c) for each p other than 2 and for a degree 3 of the "Oil and Vinegar" signature method, v is greater than n and less than or equal to n^4.

Claim 34 (previously presented): An "Oil and Vinegar" signature generating apparatus according to claim 32 and wherein a number v of "vinegar" variables is selected to satisfy the inequalities $v<n^2$ and $q^{(v-n)-1} * n^4 >2^{40}$ for a characteristic $p=2$ of a field K in an "Oil and Vinegar" scheme of degree 2, where n is a number of "oil" variables, K is a finite field from which the n "oil" variables and the v "vinegar" variables are selected, and q is the number of elements of K.

Claim 35 (currently amended): A digital signature comprising:

a signature $e_1,...,e_{n+v}$ generated by processing a set S1 of k polynomial functions provided as a public-key and a message to be signed, where the set S1 includes functions $P_1(x_1,...,x_{n+v}, y_1,...,y_k),...,$ ~~$P_1(x_1,...,x_{n+v}, y_1,...,y_k),...,$~~ $P_k(x_1,...,x_{n+v}, y_1,...,y_k)$, where k, v, and n are integers, $x_1,...,x_{n+v}$ are n+v variables of a first type, $y_1,...,y_k$ are k variables of a second type, and the set S1 is obtained by applying a secret key operation on a set S2 of k polynomial functions $P'_1(a_1,...,a_{n+v},y_1,...,y_k),...,P'_k(a_1,...,a_{n+v},y_1,...,y_k)$ where $a_1,...,a_{n+v}$ are n+v variables which include a set of n "oil" variables $a_1,...,a_n$, and a set of v "vinegar" variables $a_{n+1},...,a_{n+v}$, and the number v of "vinegar" variables is greater than the number n of "oil" variables, so that a hash function applied on the message to produce a series of k values $b_1,...,b_k$ that are substituted for the variables $y_1,...,y_k$ of the set S2 respectively to produce a set S3 of k polynomial functions $P''_1(a_1,...,a_{n+v}),...,$ $P''_k(a_1,...,a_{n+v})$ and v values $a'_{n+1},...,a'_{n+v}$ that are selected for the v "vinegar" variables $a_{n+1},...,a_{n+v}$, enable to solve a set of equations $P''_1(a_1,...,a_n,a'_{n+1},...,a'_{n+v})=0,...,$ $P''_k(a_1,...,a_n,a'_{n+1},...,a'_{n+v})=0$ to obtain a solution for $a'_1,...,a'_n$, and application of the secret key operation transforms $a'_1,...,a'_{n+v}$ into the digital signature $e_1,...,e_{n+v}$.

C1

Claim 36 (previously presented): A digital signature produced by the method of claim 1.

Claim 37 (previously presented): A method according to claim 1 and wherein said supplying comprises obtaining the set S1 from a subset S2' of k polynomial functions of the set S2, the subset S2' being characterized in that all coefficients of components involving orders higher than 1 of any of the n "oil" variables $a_1,...,a_n$

and coefficients of components involving multiplication of two or more of the n "oil" variables $a_1,\ldots,a_n$ in the k polynomial functions $P'_1(a_1,\ldots,a_{n+v},y_1,\ldots,y_k)$, $\ldots,P'_k(a_1,\ldots,a_{n+v},y_1,\ldots,y_k)$ are zero, and the number v of "vinegar" variables is greater than the number n of "oil" variables.

Claim 38 (previously presented): A method according to claim 37 and wherein the set S2 comprises a set S of k polynomial functions of a UOV scheme, and the number v of "vinegar" variables is selected to satisfy one of the following conditions:

(a) for each characteristic p other than 2 of a field K in an "Oil and Vinegar" scheme of degree 2, v satisfies the inequality $q^{(v-n)-1}* n^4 > 2^{40}$, where K is a finite field over which the sets S1, S2 and S3 are provided,

(b) for p = 2 in an "Oil and Vinegar" scheme of degree 3, v is greater than n*(1 + sqrt(3)) and less than or equal to $n^3/6$, and

C1

(c) for each p other than 2 in an "Oil and Vinegar" scheme of degree 3, v is greater than n and less than or equal to n^4.

Claim 39 (previously presented): A method according to claim 37 and wherein the set S2 comprises a set S of k polynomial functions of a UOV scheme, and the number v of "vinegar" variables is selected to satisfy the inequalities $v<n^2$ and $q^{(v-n)-1}* n^4 >2^{40}$ for a characteristic p=2 of a field K in an "Oil and Vinegar" scheme of degree 2, where K is a finite field over which the sets S1, S2 and S3 are provided and q is the number of elements of K.

Claim 40 (previously presented): Apparatus according to claim 18 and wherein the set S1 is obtained from a subset S2' of k polynomial functions of the set S2, the subset S2' being characterized in that all coefficients of components involving orders higher than 1 of any of the n "oil" variables $a_1,\ldots,a_n$ and coefficients of components involving multiplication of two or more of the n "oil" variables $a_1,\ldots,a_n$ in the k polynomial functions $P'_1(a_1,\ldots,a_{n+v},y_1,\ldots,y_k)$, $\ldots,P'_k(a_1,\ldots,a_{n+v},y_1,\ldots,y_k)$ are zero, and the number v of “vinegar” variables is greater than the number n of “oil” variables.

Claim 41 (previously presented): Apparatus according to claim 40 and wherein the set S2 comprises a set S of k polynomial functions of a UOV scheme, and the number v of “vinegar” variables is selected to satisfy one of the following conditions:

(a) for each characteristic p other than 2 of a field K in an “Oil and Vinegar” scheme of degree 2, v satisfies the inequality $q^{(v-n)-1} * n^4 > 2^{40}$, where K is a finite field over which the sets S1, S2 and S3 are provided,

a1

(b) for p = 2 in an “Oil and Vinegar” scheme of degree 3, v is greater than n*(1 + sqrt(3)) and less than or equal to $n^3/6$, and

(c) for each p other than 2 in an “Oil and Vinegar” scheme of degree 3, v is greater than n and less than or equal to n^4.

Claim 42 (previously presented): Apparatus according to claim 40 and wherein the set S2 comprises a set S of k polynomial functions of a UOV scheme, and the number v of “vinegar” variables is selected to satisfy the inequalities $v<n^2$ and $q^{(v-n)-1} * n^4 >2^{40}$ for a characteristic p=2 of a field K in an “Oil and Vinegar” scheme of degree 2, where K is a finite field over which the sets S1, S2 and S3 are provided and q is the number of elements of K.